Partners,

In advance of the tax deadline, the Internal Revenue Service today warned tax professionals of a new emerging scam in which cybercriminals obtain remote control of preparers' computer systems, complete and file client tax returns and redirect refunds to thieves' accounts.

Although the IRS knows of a handful of cases to date, this scam has potential to impact the filing of fraudulent returns in advance of the April tax deadline and is yet another example of tax professionals being targeted by identity theft criminals.

The IRS urges all tax preparers to take the following steps:

- Run a security "deep scan" to search for viruses and malware;
- Strengthen passwords for both computer access and software access; make sure your password is a minimum of 8 digits (more is better) with a mix of numbers, letters and special characters;
- Be alert for phishing scams: do not click on links or open attachments from unknown senders;
- Educate all staff members about the dangers of phishing scams in the form of emails, texts and calls;
- Review any software that your employees use to remotely access your network and/or your IT support vendor uses to remotely troubleshoot technical problems and support your systems. Remote access software is a potential target for bad actors to gain entry and take control of a machine.

Tax professionals should review Publication 4557, Safeguarding Taxpayer Data, A Guide for Your Business, which provides a checklist to help safeguard taxpayer information and enhance office security.